MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2018/2019

TSN3251 / TSC2211 – COMPUTER SECURITY

(All sections / Groups)

16 OCTOBER 2018
2.30 p.m - 4.30 p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of **NINE pages (excluding this page)** with **FIVE questions.**

2. Answer all **FIVE** questions. Each question carries **20 marks** and the distribution of the marks for each subdivision is given. Maximum allotted are **100 marks.**

3. Please write all your answers in the Answer Booklet provided.

*Answer all **FIVE** questions. Each question carries 20 marks and the distribution of the marks for each subdivision is given.* ***(5 × 20=100 marks)***

QUESTION 1:

a. Consider the following **security attacks**.

- Traffic analysis
- Masquerade
- Denial of Service (DOS)
- Repudiation

For each of the above,

(i) Give a brief description **(4×1=4 marks)**

(ii) Specify the category (passive or active) **(4×0.5=2 marks)**

(iii) Specify the security goal threatened (confidentiality or integrity or availability) **(4×0.5=2 marks)**

b. Briefly explain the differences between **'Chosen-plaintext'** and **'Chosen-ciphertext' cryptanalysis attacks**, based on 'what is known to the cryptanalyst' and the 'method used'.

(2 marks)

c. Draw and briefly explain the basic models for the following cryptosystems to provide confidentiality.

(i) **Symmetric** Cryptosystem
(ii) **Asymmetric** Cryptosystem

(2×5=10 marks)

Continued...

QUESTION 2:

a. Assume that plaintext and ciphertext characters are represented as numerical values in Z_{26} as follows:

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Answer the following questions:

(i) Assume the usage of **Hill Cipher** and encrypt the following plaintext.

coordination

Use the following key for encryption.

$$K = \begin{bmatrix} 6 & 3 & 2 \\ 4 & 10 & 6 \\ 3 & 5 & 11 \end{bmatrix}$$

(8 marks)

(ii) Assume the usage of **Affine Cipher** and assume that the plaintext '**ab**' is enciphered to '**CM**'.
Identify the key $\mathbf{k_1}$ to be used with multiplicative cipher and the key $\mathbf{k_2}$ to be used with additive cipher. **(2 marks)**

b. (i) Construct a **Playfair matrix** with the key *diligent.* **(2.5 marks)**

(ii) Using the constructed Playfair matrix, **decrypt** the following ciphertext. Assume the usage of 'x' as a filler character.

HTULGDRYRY **(2.5 marks)**

c. The encryption key in a **single stage keyed columnar transposition cipher** is given as

4 3 6 2 7 1 5

Identify the **decryption key.** **(2 marks)**

d. Find the **multiplicative inverse** of the integer (7) in ($\mathbf{Z_{180}}$) using the extended Euclidean algorithm. **(3 marks)**

Continued...

QUESTION 3:

a. With reference to **Data Encryption Standard (DES)** answer the following:

(i) Identify the **4-bit output**, if the input to S-box 1 is **100110**. **(2 marks)**

Definition of S-box 1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

(ii) Assume that the **32-bit Right Half (R_0)** obtained after passing the plaintext through the Initial Permutation Table is given as

$$R_0 = (1110\ 1101\ 1100\ 1011\ 1010\ 1001\ 1000\ 0111)_2$$

Expand R_0 using the following Expansion Permutation (E) Table to get **48-bit E [R_0]**. **(4 marks)**

Expansion Permutation (E) Table

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Continued...

b. Given the plaintext
(36 39 3C 3F 6F 6C 69 63 F3 F6 F9 FC EC E9 E6 E3)$_H$
and the key
(C6 C7 C8 C9 CA CB CC CD CE CF DF DE DD DC DB DA)$_H$

With reference to **Advanced Encryption Standard (AES)**, perform the following steps, one by one in order, with the output of one step forms the input to the next step.

(i) Show the original contents of **State**, displayed as a 4×4 matrix. **(2 marks)**
(ii) Show the value of State after **initial AddRoundKey.** **(4 marks)**
(iii) Show the value of State after **Substitute Bytes Transformation** using the table given below. **(2 marks)**

Note:

Substitute Bytes Transformation Table (AES S-Boxes)

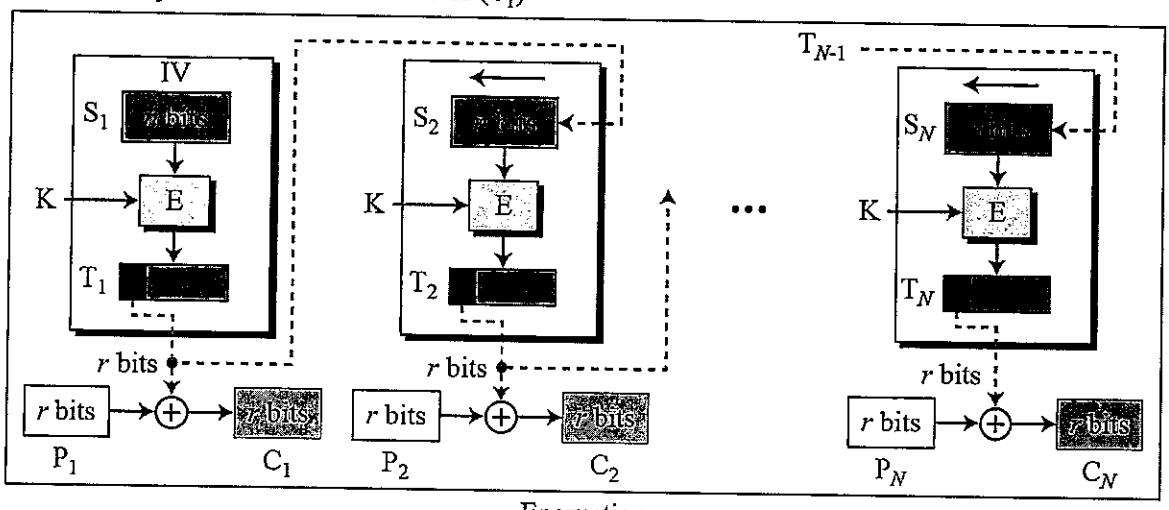
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Continued...

c. Refer the following diagram that shows the encryption and decryption process for **Output Feedback (OFB) mode** to be used with modern block ciphers for enciphering text of any size.

E : Encryption
P_i: Plaintext block i
K: Secret key
D : Decryption
C_i: Ciphertext block i
IV: Initial vector (S_1)
S_i: Shift register
T_i: Temporary register



Encryption

Answer the following questions:

(i) Briefly explain the **encryption process** with the help of the above diagram. **(2 marks)**

(ii) How will you modify the above diagram to perform **decryption process**? **(2 marks)**

(iii) Assume that there are a total of 6 blocks and bit 2 in ciphertext block 3 is corrupted during transmission. Identify the **plaintext block(s)** and the **bit(s)** affected by this. Give the reason for your answer. Assume the underlying block cipher used is AES-128. **(2 marks)**

Continued...

QUESTION 4:

a. With reference to **Rivest-Shamir-Adleman (RSA)** cryptosystem, answer the following:

(i) Identify the **public key {e,n} and private key {d,n}** for the following data using RSA_Key_Generation algorithm, as given below. **(4 marks)**

p=7; q=11; e=17

where
p and q are two prime numbers
e is an integer with gcd (φ (n) , e) =1; 1 < e < φ (n);

```
RSA_Key_Generation
{
    Select two large primes p and q such that p ≠ q.
    n ← p × q
    φ(n) ← (p − 1) × (q − 1)
    Select e such that 1 < e < φ(n) and e is coprime to φ(n)
    d ← e^−1 mod φ(n)                    // d is inverse of e modulo φ(n)
    Public_key ← (e, n)                  // To be announced publicly
    Private_key ← d                      // To be kept secret
    return Public_key and Private_key
}
```

(ii) With the help of the following algorithms, perform **encryption and decryption** using the keys derived in (i) and using the plaintext message **P=8.** **(4 marks)**

```
RSA_Decryption (C, d, n)                 //C is the ciphertext in Z_n
{
    P ← Fast_Exponentiation (C, d, n)    // Calculation of (C^d mod n)
    return P
}
```

```
RSA_Encryption (P, e, n)                 // P is the plaintext in Z_n and P < n
{
    C ← Fast_Exponentiation (P, e, n)    // Calculation of (P^e mod n)
    return C
}
```

```
Square_and_Multiply (a, x, n)
{
    y ← 1
    for (i ← 0 to n_b − 1)               // n_b is the number of bits in x
    {
        if (x_i = 1)  y ← a × y mod n    // multiply only if the bit is 1
        a ← a^2 mod n                    // squaring is not needed in the last iteration
    }
    return y
}
```

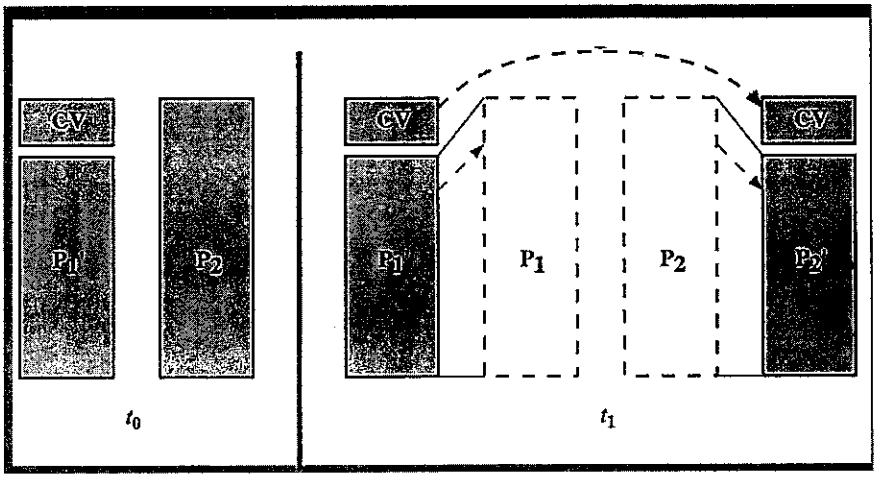
Continued...

b. State the main difference between the following with respect to 'program security'.

(i) **Computer Viruses and Computer Worms**
(ii) **Rootkits and Trapdoors**

(2+2=4 marks)

c. Assume that program P_1 is infected with the virus cv and when this program is invoked, control is passed to its virus. Briefly explain the steps involved in the **operation of compression virus logic**, which can avoid the detection of the presence of virus based on the length of the code, using the following diagram.



(4 marks)

d. Once the operating system is appropriately built, secured, and deployed, the process of maintaining security results from the constantly changing environment, the discovery of new vulnerabilities, and hence exposure to new threats. State any FOUR additional steps involved in the **process of operating system security maintenance.** **(2 marks)**

e. Briefly explain the approach of using **'hashing'** in **fixed password authentication.** **(2 marks)**

Continued...

QUESTION 5:

a. With reference to database access control, assume that the following convention is followed for **cascading authorization**:

The grant option is used to enable an access right to cascade through a number of users. If a user has an access right with grant option, the user may pass the right to another user. When user **'U'** revokes an access right, any cascaded access right is also revoked, unless that access right would exist even if the original grant from **'U'** had never occurred. Time of grant is also considered for revoking the access right.

Assume that A, B, and C grant certain privileges on the employee table to X, who in turn grants them to Y, as shown in the following table, with the numerical entries indicating the time of granting.

User ID	Table	Grantor	READ	INSERT	DELETE
X	Employee	A	15	15	---
X	Employee	B	20	---	20
Y	Employee	X	25	25	25
X	Employee	C	30	---	30

At time t=35, B issues the command REVOKE ALL RIGHTS ON Employee FROM X.

Answer the following questions based on the above convention and the given table.

(i) Which access rights, if any, of Y must be revoked?

(ii) Show the resulting **diagram of access right dependencies** after the execution of **REVOKE** command. **(4 marks)**

b. **Countermeasures** for **SQL injection (SQLi) attack** can be classified into three types: defensive coding, detection and run-time prevention. State any two **detection** methods that have been developed for this purpose. **(2 marks)**

Continued...

c. **Multipurpose Internet Mail Extension (MIME)** is an extension to the old RFC 822 specification of an Internet mail format and **S/MIME** is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. Answer the following with respect to the above protocol.

(i) State the purpose of using MIME as an extension protocol to Internet mail. **(2 marks)**

(iii) Assuming the usage of **Radix-64 conversion** method for performing content-Transfer-Encoding in S/MIME protocol, perform the encoding of the following binary data. **(4 marks)**

10000000 01000010 11111111

Identify the **equivalent codes** based on the following Radix-64 encoding table.

Value	Code	Value	Code	Value	Code	Value	Code	Value	Code	Value	Code
0	**A**	11	**L**	22	**W**	33	**h**	44	**s**	55	**3**
1	**B**	12	**M**	23	**X**	34	**i**	45	**t**	56	**4**
2	**C**	13	**N**	24	**Y**	35	**j**	46	**u**	57	**5**
3	**D**	14	**O**	25	**Z**	36	**k**	47	**v**	58	**6**
4	**E**	15	**P**	26	**a**	37	**l**	48	**w**	59	**7**
5	**F**	16	**Q**	27	**b**	38	**m**	49	**x**	60	**8**
6	**G**	17	**R**	28	**c**	39	**n**	50	**y**	61	**9**
7	**H**	18	**S**	29	**d**	40	**o**	51	**z**	62	**+**
8	**I**	19	**T**	30	**e**	41	**p**	52	**0**	63	**/**
9	**J**	20	**U**	31	**f**	42	**q**	53	**1**		
10	**K**	21	**V**	32	**g**	43	**r**	54	**2**		

d. The **Secure Electronic Transaction (SET)** is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. State the steps involved in SET for hiding the credit card details of the cardholder from the merchant. **(6 marks)**

e. State what is meant by a **security plan**? State its importance for an organization. **(2 marks)**

END OF EXAM